INFORMATION SECURITY'S CERTIFICATION AND ACCREDITATION CHECKLIST

http://www.state.nj.us/it/ps/14-13-NJOIT_205_Certification_and_Accreditation.pdf

Agency / Asset Information	
Date:	
Agency:	
ASAI:	
Project Name:	
Application Name:	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. **Check Boxes for those that are Completed**		**Initiation**	**Certification**	**Accreditation**
Business Case Review	Begin the System Architecture Review (SAR) process. http://www.nj.gov/it/reviews/forms/0133_Business_Case_Review_Template.dot			
On-Premise and/or Cloud Provider	Identify: ☐ On Premise ☐ Cloud Service Provider ☐ Hybrid. (Infrastructure as a Service – single tenant). (Software as a Service – multi-tenant with no Personal Identifiable Information or Intellectual Property).	☐		
Cloud Provider: RFP appendix requirements (including Security Plan)	http://www.nj.gov/treasury/purchase/noa/contracts/m0003_11-r-21493.shtml In addition to the Standard Terms and Conditions, please reference Amendment #3 – Change to Method of Operation. This needs to be completed by the software publisher and approved by DPP. Once the terms and conditions have been addressed, we are then able to move into the system architecture review (SAR) and security realm. We will treat the software publisher as an Business Entity. Standard Security Controls Language for RFPs – reference RFP Security Controls with Extranet & File Transfer.	☐		
Asset Classification	Completed the Asset Classification worksheet.	☐		
Security Requirements	Identified anticipated security needs based on regulatory compliance.	☐	☐	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. **Check Boxes for those that are Completed**		Initiation	Certification	Accreditation
Logical SAR	http://www.nj.gov/it/reviews/forms/0132_Logical_SAR_Template.dot			
Authentication and Access Controls	Implemented an authentication service such as State's Credential and Identity Access System. Implemented account provisioning procedures and defined access roles.		☐	
Firewall Controls	Verified and implemented firewall rule set. http://www.nj.gov/it/reviews/forms/GSN%20Extranet%20Firewall%20Form.dot		☐	
Business Entity or Extranet: Appendix A, B, C, and D	Completed the Business Entity and Extranet Appendices. http://www.state.nj.us/it/ps/09-11-NJOIT_Extranet_Policy.pdf		☐	
A. Application Form. http://www.state.nj.us/it/ps/09-11-P1-NJOIT_0110%20GSN%20Extranet%20Application%20Form_Appendix_A.pdf			☐	
B. Memorandum of Understanding. http://www.state.nj.us/it/ps/09-11-NJOIT_0184_Business_Entity_IT_Services_Extranet_%20MOU_Appendix_B.dot			☐	
C. Operational Form. http://www.state.nj.us/it/ps/09-11-NJOIT_0145_Business_Entity_IT_Services_Extranet_Connection_Detail_Appendix_C.dot			☐	
D. Security Controls Assessment Checklist. Documentation is available through SOIS (njinfosecure@oit.nj.us) request or NJ-ISAC			☐	
Encryption	The data is encrypted in transit.		☐	
	The data is encrypted at rest.		☐	
PCI-related application	PCI certification (Attestation of Compliance). The Attestation is a PCI-DSS assessment and certification of the Business Entity's PCI security requirements performed by a security representative (Qualified Security Assessor). A copy of the Attestation of Compliance has been provided.		☐	
Data Transfer	An interface report has been completed and workflow established.		☐	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. **Check Boxes for those that are Completed**		Initiation	Certification	Accreditation
DOTGOV name space	Create the dotgov name space space (include other domain space .com, etc) within the State's environment. In order for a DOTGOV to be acquired by a state level authority the Chief Information Officer must approve the domain via a signed authorization letter. Creative Services keeps a copy of all the authorization letters. OIT does not pay for any client domains. All domains are registered by the client at their respective registrar; nj.gov and state.nj.us are registered through OIT.		☐	
Physical SAR	http://www.nj.gov/it/reviews/forms/0135_Physical_SAR_Template.dot			
Vulnerability Assessment	http://www.state.nj.us/it/ps/12-04-NJOIT_201_Vulnerability_Management.pdf		☐	
	Requests to OIT for a vulnerability assessment of applications, hosts, devices or networks should be submitted to oit.riskassessments@oit.nj.gov no later than 4:00 pm Thursdays and prior to 20 business days before production. Execution of security scanning will be conducted the next week following the request. The risk assessment and remediation are not included in the scanning process and must be factored into the project timeline.			
	1) OS and Software scans.			
	Scan Date		☐	
	Requestor Name			
	2) Application security scans.			
	Scan Date		☐	
	Requestor Name			
	3) Penetration testing.			
	Scan Date		☐	
	Requestor Name			
	Vulnerabilities Detected. ☐		☐	
	Vulnerabilities Results Reviewed. ☐			
	Vulnerabilities Report Distributed. ☐			
Risk Assessment	http://www.state.nj.us/it/ps/14-02-NJOIT_Risk_Management.pdf		☐	

The purpose of the checklist is to guide an agency and for the Statewide Office of Information Security to follow in validating security requirements for systems, applications, system software, and other technologies before they are deployed into a production environment. It is designed to ensure compliance with specifications, regulations, standards and objectives identified during each phase of the System Development Life Cycle (SDLC). Reference the 205 – Certification and Accreditation Policy. **Check Boxes for those that are Completed**				**Initiation**	**Certification**	**Accreditation**
Risk Management Remediation Report Template	http://www.state.nj.us/it/ps/0166_Risk_Management_Remediation_Report%20Template.xls				☐	
	Date Risk Remediation Rpt. Distributed:		**Report Distributed**	☐		
	Risk Remediation Rpt. Distributed to:					
	Date Risk Remediation Rpt. Returned:		**Report Returned**		☐	
Logging / Audit	Implemented logging and auditing requirements. Reference minimum audit log requirements found in 171-01-Minimum System Security and Protection Standards.				☐	
Minimum System Security	Implemented security requirements. http://www.state.nj.us/it/ps/14-01-NJOIT_171_Minimum_System_Security_Requirements.pdf 1) Harden the OS and software. CIS Security Benchmark tools. https://benchmarks.cisecurity.org/en-us/?route=default 2) Patch Management. 3) Anti-malware and Intrusion Detection.				☐	
Email Relay	The State system is using the State's email relay and content inspection system.				☐	
Privacy and Disclaimer	Added the standard privacy and disclaimer notices to the State's system.				☐	
DOTGOV Address Assignment	Redirect the purchased name space to the DOTGOV IP address.				☐	
Exception:	Received an exception request(s). http://www.state.nj.us/it/ps/08-02-NJOIT_Policy_Exception_Request_Form.pdf				☐	
Implementation Review	http://www.state.nj.us/it/reviews/forms/0134_Implementation_Review_Template.dot					☐

Please submit the Certified Accreditation Checklist to njinfosecure@oit.nj.gov at the same time your Implementation Review is submitted to sar@oit.nj.gov.